University of Technology, Sydney

Event Management of Large Distributed System and Network Management Environments

Antony Gavin James Parsons

Thesis in fulfilment of the degree of Ph.D. (Computing Sciences)

28th July 2006

CERTIFICATE OF AUTHORSHIP/ORIGINALITY

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of Student

.....

Acknowledgements

This thesis could not have been written without the support of others.

The first person to be "mentioned in dispatches" is my supervisor, Bruce Howarth. Without him this thesis would not have been possible. I would like to thank him for his ideas and suggestions throughout the development of this thesis. I would also like to thank him for all the hours of proof reading while I wrote this thesis, and for continuing to be my supervisor even as he entered retirement. It was Bruce that ruthlessly removed split infinitives, verbalised nouns and inappropriate apostrophes, as well as gently persuading me to shed the excess baggage of an overweight first draft.

I would like to thank the team of Reid Purvis, Jarra Voleynik and Tom Spudic who helped me make the first practical part of the thesis such a success, and I would like to thank Matt Fitzgerald and Nick Tamburro who greatly assisted in subsequent work in the implementation of the thesis.

Naomi Sweeney deserves a special mention for all the countless hours she saved me by helping on the formatting and editing of the thesis.

I would also like to thank my employer, Hewlett-Packard for providing me with the time and resources that I required for this thesis.

Finally, I wish to thank my wife, Alison, as well as my daughters Lizzie and Alex – who both came along during the thesis – for putting up with the inconvenience of having my study slowly grow through the house as the thesis approached completion!

Table of Contents

List of Figures

List of Tables

Abstract

Co-ordinated event management across system, network and application environments is a challenging task. The wide diversity of industry and commercial standards, differing business and technical requirements and a huge variety of environments mean there are no simple solutions. This thesis proposes a highly scaleable, flexible and resilient event management architecture that has been applied to the outsourcing activities of HP Services worldwide.

Our solution is based on industry standards such as SNMP and commercial products. It provides a framework for all aspects of event management, including event detection, logging, notification, and correlation. It was initially applied and refined in an outsourcing IT environment, then further developed in larger outsourcing environments. It was developed using a standard solution architecture methodology (known as ITSA) that enabled the partly developed architectures to be continually refined, improved and deployed. The technology aspects of the solution work closely with ITIL event management processes.

To achieve a unified event display and a standardised event message format, all events from all sources are reduced to a standard format that includes the "raw" event information plus business intelligence, called the *business string*, added to the event for display and routing purposes. This extra information identifies the nature of the event and allows filtered displays of events. It is extracted from configuration management extensions added to the standard event management tools. The extended format is flexible enough to handle the different commercial tools.

The first generation of the solution was based on Computer Associates' Unicenter TNG and was called the Event Monitoring Utility (EMU). This was later significantly extended by switching to HP OpenView, and the extra development of further central event management functions, especially event correlation, in a solution called DECADE.

Significant agent extensions were achieved by the creation and deployment of a solution called SMSPI, which included an extended configuration management and policy database, and further event automation.

The extended solution is now deployed across HP Services' entire global outsourced environment. The solution has proven very successful, winning two Computer Associates Software Achievement Awards, including the Grand Prize, and generating two US patents. It will be progressively deployed to several million servers and network devices globally over the next few years.

The work described here is at once self-contained and a basis for on-going development of event management in the face of ever more complex systems, and increasing demands for more detailed event management.